Paso Robles JUSD
Exhibit

E 4040
Personnel

Employee Responsible Use of Technology

COMPUTER AND NETWORKED INFORMATION RESOURCES
RESPONSIBLE USE AGREEMENT FOR STAFF MEMBERS

Paso Robles Joint Unified School District recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills. To that end, we provide access to technologies for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally-owned devices on the school campus. Before using on-line services, PRJUSD staff shall sign the district's CIPA (Children's Internet Protection Act) Compliant Acceptable Use Policy indicating that the PRJUSD staff member understands and agrees to abide by specified user obligations and responsibilities

Usage Policies
All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; staff shouldn't try to get around technological protection measures; use good common sense.

Technologies Covered
PRJUSD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. As new technologies emerge, PRJUSD will attempt to provide access to them. The policies outlined in this document are intended to cover *all* available technologies, not just those specifically listed. This includes Personal Electronic Devices when allowed through this policy.

Network Conduct/Acceptable Use:
The Paso Robles Public Schools' computer system is expected to be shared and available to all **approved** users. The computer system then may not be used in such a way as to disrupt or interfere with its use by others. Inappropriate conduct in the use of the system includes, but is not limited to the following:

* Damage, vandalism or theft of equipment
* Theft, piracy or altering of software

* Installation/Downloading/Utilization of unauthorized/unapproved software including filesharing (eg. Kazaa) software
* Theft of services
* Use of the system to communicate unlawful information or to transmit computer viruses
* Accessing information which is pornographic, obscene, sexist, racist or abusive
* Plagiarism of ideas or information
* Violation of copyright law
* Use of the system for commercial purposes or for political campaigning
* Assuming another person's identity on the network (e.g. using a login/password that is not the user's).
* Attempting to gain and/or Subvert/Bypass PRPS' computer security/file management system
* Not using the PRPS' assigned login/password during any computer use
* Attempting to gain unauthorized access to the PRPS Network
* Making deliberate attempts to disrupt computer system or network, destroy computer data, or physically modify, harm, or destroy any computer or network hardware
* Utilization of file sharing software to obtain copy protected/copyrighted/ inappropriate files.
* Attempting to vandalize equipment and/or harass other users. Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user, which includes, but is not limited to, the loading or creating of computer viruses. Harassment is defined as the persistent annoyance of other users, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted e-mail
* Any violations of the classroom rules, school conduct code, Educational Code or Penal Code

Netiquette

Users are expected to always use the Internet, network resources, and online sites in a courteous and respectful manner. Users are expected to use trusted sources when conducting research via the Internet. Users are also expected to remember not to post anything online that they wouldn't want parents, students, district staff and our community to see. Once something is online, it's out there—and can sometimes be shared and spread in ways never intended.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Staff is expected to notify the district Technology Department if a computer or mobile device that is being used might be infected with a virus. The Paso Robles Public Schools' computer system is intended for the exclusive use of its registered users who are responsible for their password and their accounts. Any problems that arise from the use of the account are the responsibility of the account holder. Any misuse of the account or system will result in disciplinary action and/or the suspension or cancellation of privileges. Use of the account by someone other than the registered user will be grounds for cancellation and will result in disciplinary action. Any user identified as a security risk for having a history of discipline/appropriate use problems with other computer systems will be denied access to PRPS Workstations and the Internet by the Paso Robles Public Schools.

The Paso Robles Public Schools' computer system is intended for the exclusive use of its registered users, who are responsible for their password and their accounts. Any problems which arise from the negligent use of the account are the responsibility of the account holder. No staff member should log into any PRPS network/workstation using another staff member's account information.

Classrooms have access to networked student records, security of those records is paramount. Consequently, no students are allowed to enter, import, export, or view information from the PRPS Student Data Management System (e.g. Aeries). Staff members must not leave a logged-in computer with Aeries/gradebook opened on the screen.

Personal Safety
Users are expected to never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users are expected to recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.

Plagiarism
Users are expected not to plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Email
PRJUSD may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. If users are provided with email accounts, they are expected to be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.
Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content
Recognizing the benefits collaboration brings to education, PRJUSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate,

safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users are expected to be careful not to share personally-identifying information online.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Social Media Guidelines

Educators have a professional image to uphold and how they conduct themselves online helps determine this image. As reported by the media, there have been instances of educators demonstrating professional misconduct while engaging in inappropriate dialogue online (i.e. blogs, wikis, social networks, texting, instant messaging) about their schools, colleagues, and/or students or posting pictures and videos of themselves engaged in inappropriate activity. The following guidelines are intended to serve as a reference for all District personnel who elect to engage in social media, regardless of whether such online activity occurs during working or non-working time. If any employee is uncertain about how to apply these guidelines or have any question about participation in social media, they are expected to seek the guidance of a supervisor or other appropriate district administrator. When participating in social media, personnel are bound by the following guidelines:

- Do not initiate online "friendships" with students or accept students as "friends" on personal social networking sites. Decline any student-initiated "friend" request. Remember that anyone classified as a "friend" has the ability to download and share your information with others. Only District-endorsed networking platforms, such as *SchoolCenter and Moodle*, which have restricted access, may be used to engage with students for educational purposes.
- Do not use language that could reasonably be perceived as defamatory or obscene.
- Exercise caution with regards to exaggeration, colorful language, guesswork, and conclusory statements.
- Do not post any material that should not be seen by students, parents, or school administrators.
- Do not discuss students or personnel. Do not identify students or personnel by name or use other identifying information. Do not criticize school policies or personnel. Do not post images of students

Internet Access / Monitoring

It is possible that there is material on the Internet that is objectionable and not educationally relevant. Staff members will supervise student computer use and student Internet use, and will take appropriate action if student computer misuse is discovered. Although your students' use of the Internet is supervised by you, the instructor, and Internet firewalls and filters are employed, the District cannot guarantee that your students will not gain access to inappropriate material. The District provides a software-based system to assist teachers in selecting, blocking and monitoring Internet sites as well as training for staff using Internet sites. The District reserves the rights to any materials stored in files which are generally accessible to others and will remove any material that is believed to be unlawful, obscene, pornographic, abusive, or otherwise objectionable. The system may not be used to obtain, view, download, or otherwise gain or provide access to such materials. The District staff will refer for disciplinary action any individual who does not comply with the provisions of this agreement. Cancellation of user privileges and possible personnel action will be at the discretion of the District after application of due process.

Mobile Devices Policy

PRJUSD may provide users with mobile computers or other devices to promote learning outside of the classroom. Users are expected to abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users are expected to report any loss, damage, or malfunction to district IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

Personal Electronic Devices (PED)

PED Introduction and Definition

This policy relates to any personal electronic device (PED) that could be used for communications or data storage and retrieval. This includes, but is not exclusive of mobile phones, USB drives, MP3 players, PDAs, laptop computers, tablet computers, DVD players, and calculators. PRJUSD embraces emerging digital technologies and encourages its teachers and students to look for ways of using them to enhance teaching and learning. The technology of mobile phones and other electronic devices to facilitate the recording of sound, take photographs and video images is open to abuse, that can lead to an invasion a of person's privacy. The availability and appropriate use of these resources provide opportunities that can help students develop spiritually, academically, socially and physically. Their inappropriate use can be detrimental to the teaching / learning process, anti-social, and even harmful. PRJUSD will be providing wireless network access for PEDs to some of our educational and school sites. Network access for PED equipment will only be allowed via wireless Ethernet technology, not via direct Ethernet structured cabling in district facilities. As sites become online, we'll inform staff on wireless connecting procedures. PRJUSD will not be held responsible for the loss, theft or destruction of any personal electronic devices. PRJUSD reserves the right to review files on any mobile device brought into a school. The Computer and Network Information Resources Acceptable Use Agreement for Staff also applies to all personally-owned electronic devices. Any violation of these rules will result in the loss of the staff's privilege to bring mobile electronic devices to a district or school facility.

PED Policy for Non-wireless Sites
Because of security concerns, when PEDs are used on campus, they are expected not to be used over the school network without express permission from district IT staff.

PED Policy for District Wireless Sites
For PEDs that connect to the school wireless network:

- Staff should use PEDs for positive purposes: for learning, professional development and for legitimate communication.
- PEDs must not be used to harass or victimise other students or staff, or to abuse a person's right to privacy (for example, taking, storing and then using a digital photo/video without a person's permission).
- The device is to be running the latest Virus Protection software including the latest weekly virus definition files.
- The device is to be running the latest Security Patches for its Operating Systems.
- The device is to be free of spyware, adware, worms, viruses, trojan horses, and peer to peer software that could disrupt the network.
- The device is not to be used for any illegal activity, peer-to-peer file sharing (including Kazaa, Limewire, Gnutella, Napster, Bit Torrent, etc...), hacking or cracking this network or any other, downloading large files, or viewing (or listening to) streaming media.
- The device is not to be running any Internet or web hosting services and is not to have Internet Connection Sharing services turned on.
- During school operation hours, the internet may only be accessed through the school site wireless network, not through any other Internet access
- In using their PEDs, staff are expected to comply with the Computer and Networked Information Resources Acceptable Use Agreement for Staff.

No Warranties
The Paso Robles Public Schools will not be held responsible for the loss of data resulting from delays, non-deliveries, or service interruptions sustained or incurred in connection with the use, operation, or inability to use the system. The District specifically denies any responsibility for the accuracy or quality of information obtained electronically. Use of any information obtained electronically is at the risk of the user. While PRJUSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. PRJUSD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Encounter of Controversial Material
The Internet, a community of network systems, is not governed by any entity. The District does not have control over the kind or quality of information that is accessible to Internet users. Although the District does utilize Internet content filtering technologies to provide an academic computing environment, it is the responsibility of the staff member/user to utilize networking technologies for obtaining solely academic and educationally appropriate content.

Equipment

Staff members are responsible for the proper use of the equipment in their office space or classroom.

Installing Software

PRPS is cognizant that educators need to install software on their classroom workstation(s) in order to meet student needs. In order to help insure that installed software will not render the computer and/or the PRPS Wide Area Network (WAN) inoperable, and to insure that PRPS stays within software licensing agreements, please do the following prior to installation:

Call or email the TechGroup/CERF and convey the following information:

- Educator's Name
- Location of Computer(s)
- Location of the software CD/DVD that is to be installed.

Information & Technology department may refer the software to the Technology Advisory Committee and the Department of Instruction for review. Information & Technology maintains base computer "images" or software loads for each model computer. There must be a "compelling instructional need" for adding software to a computer's base image.

No Expectation of Privacy

The computer system provided by Paso Robles Public Schools is the property of the schools. No person using the system has a right to expect privacy with respect to any material stored on that system, including email and material downloaded from the Internet. The District reserves the right to monitor and access all such material.

Penalties for Improper Use

Any user violating rules, applicable to state and federal laws, or posted classroom and District rules, is subject to loss of network privileges and other disciplinary actions. In addition, pertaining to State and Federal laws, any unauthorized access, attempted access, or use of any state computing and/or network system is a violation of Section 502 of the California Penal Code or applicable federal laws and is subject to criminal prosecution.

PLEASE RETAIN THIS PAGE FOR YOUR FILES

ExhibitPASO ROBLES PUBLIC SCHOOLS
version: February 22, 2000 Paso Robles, California
Revised March 8, 2011